Problem Set 2 Solutions

**Problem 5.** Alice shuffles a deck of 52 cards and deals it out to herself and Bob so that each gets half of the cards. Alice now wants to send a secret message $M$ to Bob. Eavesdropper Eve is watching and sees the transmissions.

*Part A.* Suppose Alice’s message $M \in \{0, 1\}^{48}$ is a string of 48 bits. Describe how Alice can communicate $M$ to Bob in a way that achieves perfect privacy.

There are $N = \binom{52}{26} \approx 2^{48.82}$ ways to deal out the cards. Arbitrarily number the hands Alice might hold 0, 1, \ldots, $N - 1$. Alice and Bob both know Alice’s hand, so regard it as a shared key $K \in \mathbb{Z}_N$. Now regard the 48-bit string $M$ that Alice wishes to send as a number $M \in \mathbb{Z}_N$. (We can do this since $0 \leq M < 2^{48} < N$.) Alice encrypts $M$ to the ciphertext $C = (M + K) \mod N$. The distribution on $C$ is then uniform over $\mathbb{Z}_N$ because $K$ is uniform on this set.

*Part B.* Now suppose Alice’s message $M \in \{0, 1\}^{49}$ is 49 bits. Prove that there does not exist a protocol that allows Alice to communicate $M$ to Bob in a way that achieves perfect privacy.

Now we have $2^{49}$ possible messages but $N = \binom{52}{26} < 2^{49}$ possible keys. Choose an arbitrary key and let $C$ be the ciphertext of $M = 0^{49}$ under this key. Perfect privacy means that the distribution of this ciphertext must be independent of the value of the plaintext. But when we try to decrypt $C$ under every possible key, there are at most $N$ possible plaintexts, so some plaintext $M'$ never yields $C$ as the ciphertext. In other words, the adversary Eve does learn something from the ciphertext $C$: she learns that the plaintext of $C$ is not $M'$. This violates perfect privacy.